LA-UR-96-3938

Title: **The Real Deal on Seals Improving Tamper Detection**

Author(s): R.G. Johnston

Submitted to:

http://lib-www.lanl.gov/la-pubs/00418795.pdf

Los Alamos
NATIONAL LABORATORY

Form No. 836 R5
ST 2629 10/91

LAUR #96-3938

The Real Deal on Seals

Improving Tamper Detection

Roger G. Johnston, CPP

Introduction

In the spring of 1996, a senior member of a federal agency visited Los Alamos National Laboratory, having heard of work its Vulnerability Assessment Team had done on tamper-indicating devices. The official told the team that he had been using dozens of different types of these devices, also known as security seals, to protect personnel records, ensure physical security of computer components, seal rooms to prevent bugging, and to protect many other agency assets. The official was shocked to learn that the lab team was able to defeat every one of the seals tested, ranging from low-tech adhesives to high-tech fiber-optic seals, within a matter of minutes. Some seals could be opened and repaired cosmetically with little sign of tampering.

Nonplussed, the official asked about available products that could not be defeated. The hard truth, he was told, is that no such devices exist.

Security managers should not, however, avoid security seals simply because they can be defeated. Used properly, they can play an important role in overall security.

Testing

The Vulnerability Assessment Team (VAT) at Los Alamos National Laboratory has evaluated nearly 100 different security seals. These seals were developed by both industry and government, and range from simple seals costing a few cents per unit to complex and expensive electronic devices. Most are in widespread use, often for critical applications.

The bad news for users is that the VAT has devised and demonstrated rapid, inexpensive, low-tech ways to defeat all seals that it has evaluated, and virtually

anybody can do it with practice. ("Defeating" a seal means gaining entry without being detected.) Defeat times ranged from three seconds to two hours, depending on the seal. The average defeat time was four minutes.

Defeat times reflect the time it took a single person proficient at attacks to defeat the seal. For some seals, defeat time was cut markedly when one or more persons assisted in the attack.

The low-tech strategies the team has developed use simple, homemade custom tools as well as standard tools and materials readily available from hardware stores, tool companies, model railroading catalogs, and medical and dental supply companies. These techniques can involve manipulating and picking the seal to open it without damage, drilling tiny holes for manipulating the seal interior, or using thermal or chemical attacks to weaken adhesives or printing inks. They can also include cutting the seal off and repairing or hiding any damage when it is resealed, using electronic devices to spoof the seal, or counterfeiting the seal or part of the seal. Brute force or high-tech methods are not necessary.

For some of the approaches the team has demonstrated, there appears to be no way to detect that the seal has been beaten. With others, the defeat can be detected only if the seal is disassembled and carefully examined. Most of the attacks, however, can be detected externally, but only if the inspector is aware of specifically what to look for in each type of seal.

The VAT vulnerability assessment of security seals, as well as the team's experience in examining different security programs, has revealed ways to improve seal security, which can help security managers use them effectively.

Once an organization decides to put seals in place, it must understand seal basics and organizational objectives, choose the right seal for its application, optimize the seal's use, adequately protect the seal and seal data, provide effective training and support for seal inspectors, and honestly evaluate vulnerabilities.

Seal Basics

Tamper-indicating devices are widely used in industry, government, and the consumer world to detect unauthorized attempts to open a container. Whether a piece of foil on a jar of peanut butter or a fiber-optic loop on a radioactive waste container, seals are intended to leave unambiguous, nonerasable evidence of unauthorized access. Seals are used for many different applications including access control, records integrity, inventory, shipping integrity, theft prevention and detection, hazardous materials accountability,

nuclear nonproliferation, national defense, law enforcement, customs, counterterrorism, counterespionage, and consumer product protection.

Seals take a variety of forms. They can be frangible foils or films, plastic wraps, pressure-sensitive adhesive tapes, crimped cables or other (theoretically) irreversible mechanical assemblies; security containers or enclosures that give evidence of being opened; devices or materials that display irreversible damage or changes when manipulated; and electronic systems (reminiscent of burglar alarms) that continuously monitor for changes, such as a break in an electrical cable or fiber-optic bundle.

Understanding Goals

Many seal users are remarkably vague about what they are trying to accomplish. Seal security cannot be effectively implemented, or optimized, without clear answers to these questions: What is the organization trying to protect and why? What are the costs and consequences when security fails? What changes can be made to improve security for the least cost and hassle? What resources (time, energy, personnel, money) is the organization willing to devote to tamper detection? Who are the organization's adversaries? What resources are they likely to have available?

Goals should be periodically reviewed to ensure that they are current, clear, and appropriate. The security team should ensure that its methods change as the organizational goals and situations change.

Seal Selection

Once needs are fully analyzed, security managers should choose a seal that is appropriate for the application and desired level of security. Many seal users choose a seal based primarily on unit cost--often the least important economic factor. Costs associated with additional hardware, seal training, paperwork, installation, inspection, and removal can be far more important than the seal purchase price.

It is important to choose tamper-indicating products carefully. Considerable confusion exists among some security professionals about whether they should be using a lock, a seal, or a tag. A lock provides a physical barrier that delays entry. A seal often provides little or no barrier, but is intended to leave evidence behind that entry took place. A tag is meant to uniquely identify an object so that it can be recognized at a later date, or so that it won't be confused with a different object that looks similar.

The question of lock versus seal versus tag can get confusing--most security products have some attributes of each. A padlock, for example, while primarily a lock, can provide evidence of entry if it has been drilled, sawed, or smashed open. Similarly, a seal can sometimes serve as a tag since the seal will theoretically indicate any effort to remove it and place it on a different object. To be effective, all seals must have a tag-like "fingerprint," or unique identifier, such as a serial number. Otherwise, an adversary can simply cut off the seal and replace it with an unused one.

The VAT's experience at Los Alamos suggests that hybrid products are frequently ineffective. If, for example, a user wants both a physical barrier to entry AND tamper detection, the team suggests using a good lock in conjunction with a good seal, rather than a single hybrid product that may perform neither function particularly well. Hybrid products sometimes have a tendency to add to users' confusion about what they are trying to accomplish.

What kind of seals are best used in specific applications? Factors vary, but general rules of reason apply. For example, doors on railroad cars and trucks need robust protection because of their size and weight as well as their propensity to be heavily jarred in transit. Common choices for these vehicles include metal ribbon, cable, and bolt-type seals.

On the other end of the spectrum is protection of small containers such as blood vials or urine specimen bottles for drug testing, which calls for a lightweight, easy-to-use device, such as wire-type seals and pressure-sensitive adhesive seals. In all cases, who the user is and what the threat is dictate what type of seal is most appropriate.

Seal Protection

Many seal users are careful to safeguard their seals prior to use but careless about disposing of used seals and seal parts. This sloppiness can be exploited by an adversary intent on learning about an organization's seal program, getting sample seals and components to practice defeat techniques, and counterfeiting seals, seal parts, serial numbers, or imprinted/stamped logos.

Once a seal has completed its function, it should be protected or thoroughly destroyed. Punching a hole in the seal or cutting it in half is not sufficient. If practical, the security manager should consider storing used seals for possible future forensic analysis when new attacks or problems are discovered.

Recorded data about an applied seal, such as its serial number, color, photograph, or stored electronic information, must also be well-protected from

tampering. Seal users should not store the seal serial number (unless encrypted) on paperwork kept inside or alongside the container that the seal is protecting. An adversary can simply replace the original seal with a seal having a different serial number after modifying the paperwork inside the container.

Inspection

The single most critical issue associated with seal security is the inspection process. Some seal users and potential users don't understand that seals can only detect tampering if they are inspected. (Locks, in contrast, provide security even when ignored.) Seal inspection is sometimes done automatically by electronics or a computer system, but for most seals, the inspection is performed manually.

Even a simple, inexpensive seal can provide effective security if properly inspected. On the other hand, highly sophisticated, expensive seals may provide remarkably poor tamper protection if the inspection protocol is ineffective.

Training

For optimal tamper detection, the VAT believes it is crucial that seal inspectors be trained in the most likely attack scenarios for each seal they use, and that inspectors specifically look for signs of those attacks. For example, many seals can be opened and resealed to look like they did before being compromised. Unless inspectors have seen actual examples of seals that have been reapplied after attack, they can easily miss the subtle signs of cosmetic alteration. Such signs include discoloration, scratches, and gloss differences.

Some seals are inspected by doing, an on-site visual comparison of before and after photographs of the seal. Differences are indicative of tampering. For such seals, the Los Alamos team, recommends use of a "blink comparator," which seal inspectors should be trained to use. This is a simple and in-expensive device that overlays the reflected image of one photograph on the image of another photograph, flashing back and forth between the photos two to forty times a second, giving the impression that the pictures overlap. Any differences between the two images are immediately detected by the brain and interpreted as movement. A blink comparison can also be done on a computer monitor.

Inspectors should be trained and encouraged to think on the job rather than mindlessly follow a formal inspection procedure. Security managers should encourage candid input from seal inspectors and review and acknowledge it.

It is particularly important to avoid a "kill the messenger" environment. In many security programs, inspectors are hesitant to report evidence of tampering, because of the anxiety it creates for security supervisors. Often the inspector is blamed for creating the problem or making the boss took bad.

Inspectors, as well as all other security personnel, should always be treated with consideration and respect. Having disgruntled security personnel is a classic way that security programs fail.

To the extent practical, seal inspectors should be engaged intellectually and emotionally in the task of catching the bad guys. Contests and prizes might be offered for finding compromised seals in actual use or during training exercises.

Vulnerability

All security programs and security seals should undergo periodic vulnerability assessments. Ideally, these will be conducted by independent outside evaluators who are experienced in finding problems and suggesting solutions. The security manager should not accept a finding of no vulnerabilities; that situation does not exist.

If the cost or security concerns prevent the use of outside evaluators, alternatives are available. Security managers can draft evaluators from within their own organization. Ideally, these should include clever, hands-on people with no direct involvement in the security program and thus no preconceived notions about security issues. It is remarkable how often nonexperts can spot problems that have eluded security personnel caught up in the day-to-day details of the job. This kind of activity also pays benefits by improving security awareness throughout the organization.

The security manager should encourage in-house security personnel to think about how they would defeat the company's seals. The mental exercise of thinking like an adversary can raise awareness and reveal vulnerabilities.

Security managers should view the discovery of any vulnerabilities as good news. Vulnerabilities always exist. Identifying them and taking appropriate counter-measures builds confidence and improves overall security.

Seal Designs

Most of the seals that the Vulnerability Assessment Team has evaluated would, in the team's view, be greatly improved by changes in design. In many cases, the changes the team suggests are minor and low-cost. Some of the recommended design modifications are common to a number of different seals. Other recommended changes depend on the specific seal and application.

One typical problem is lack of a serial number on the seal, or the use of a serial number on only one seal component. (For instance, a bolt seal has two pieces: a bolt body and a head that snaps onto it. It is common for manufacturers to place a serial number on the head but not the body of the bolt.) The VAT believes it is important to place a serial number (ideally the same) on all independent components of the seal. This step makes it more difficult for an adversary to replace the seal or its components with parts from another seal made by the same manufacturer.

When serial numbers or customized logos are embossed or stamped onto a seal, the process should be done deeply. For many seals, the embossing or stamping is so shallow that it can easily be buffed off and replaced.

In the case of pressure-sensitive adhesive tape or label seals, it is crucial that the adhesive, printing ink, and the substrate material be soluble in the same solvents to the extent practical.

Currently, many adhesive seals can be removed easily from a surface by dissolving the adhesive in the right solvent, one that does not damage the substrate, printed serial number, logo, or patterns. Ideally, the adhesive should also be designed to melt at a higher temperature than the printing ink or substrate material.

There is no such thing as an undefeatable seal. Assurances from manufacturers or sales personnel that their seals are tamper proof should be ignored. In some cases, using a security seal may actually decrease overall security if the user naively trusts the product. At best, security seals should be considered as only one part of an overall security program. The security manager should bear in mind that the most successful tampering, often completely bypasses any security seal, such as when the back of a container is pried open.

It is always important to focus on the weakest link in the chain of security. High-tech security systems or products are particularly vulnerable to over confidence and focus on the wrong issues. They can often be defeated with simple low-tech, physical attacks that require little sophistication, time, or skill. Developers and end users of high-tech systems may well be experts on

electronics and computer security, but they frequently have limited experience with physical tampering.

Like many security devices, seals have their place. Users of locks, safes, and vaults, for example, generally accept that they provide less than absolute protection against unauthorized entry. Similarly, seals do not have to be absolutely tamper proof to be useful

Even inexpensive, easily defeated seals can provide a powerful psychological impediment to tampering in the minds of casual and novice adversaries. They can also serve to focus attention in the minds of security personnel, employees, and customers on tampering concerns.

Security managers should therefore balance the knowledge that no seal is perfect with an awareness of the role these devices can play. If used with proper care and inspections, seals can prove a useful tool in any security program where unauthorized entry is an issue.

Appendix/Sidecar - Sticking Points

Pressure-sensitive adhesive tape or label seals are popular because of their low cost and ease of use--they can be found on everything from file cabinets to small vials and bottles. They do not generally provide high levels of security; however, their ability to detect tampering can be optimized in several ways.

Adhesive seals should only be used when the application's temperature extremes and the nature of the surfaces for adhesion are taken into account. One common problem is that surfaces undergoing temperature changes often experience condensation, which may interfere with adhesion. Unfortunately, there is no rule of thumb because it's difficult to predict which surface an adhesive will work well on.

One thing to be wary of, however, are product demonstrations by vendors. Sales people might bring in a surface that the adhesive sticks to solidly, but it may be a special surface or one that is coated or painted a certain way. The most prudent method of selecting an adhesive seal is to analyze the makeup of the seal and consider the temperature ranges it works in (taking into account temperatures from the point the seal is applied until the protection job is done). Then try the seal on the container that needs to be protected.

If adhesives are to be used, the user should thoroughly clean the surface prior to applying the seal. The security team should be alert to signs of pre-oiling or coating of the surface, particularly if an adversary knows in advance where the seal is to be applied. Pretreating a surface can dramatically

decrease adhesion and make it easy for an adversary to remove and later reapply the seal.

Adhesive seals should ideally be well protected for the first twenty-four to forty-eight hours after being applied, which allows time for significant adhesion to occur. Many adhesive seals are easy to remove from even a clean surface prior to this time. Heat can sometimes help speed up the adhesion process.

When an adhesive seal is inspected visually, it should be compared with an identical seal held alongside. Humans have poor memory of exact color, dimensions, textures, gloss, and patterns, but can easily spot subtle differences in a side-by-side comparison.

The inspection should include a careful examination of the edges of the seal and the surface outside the seal perimeter. Also, any portion of the adhesive seal that did not originally adhere to the surface, such as a part of the seal over a slot or a screw hole, should be carefully examined.

About the Author

Roger G. Johnston, CPP, Ph.D., has been a team and project leader in the Chemical Science and Technology (CST) Division at Los Alamos National Laboratory since 1985, where he is the team leader of the Los Alamos Vulnerability Assessment Team. He is a member of ASIS. The work of the Los Alamos Vulnerability Assessment Team is performed under the auspices of the U.S. Department of Energy. Anthony Garcia, Kevin Grace, and Janie Enter provided useful input for this paper.